Before the

Federal Communications Commission

Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate	)	CG Docket No. 17-59
Unlawful Robocalls	)	

Reply Comments of AARP

August 23, 2019

Trevor R. Roycroft, Ph.D.
Economic Consultant

David Certner
Legislative Counsel and
Legislative Policy Director
Government Affairs
AARP
601 E Street, NW
Washington, DC 20049

Table of Contents

Introduction

AARP respectfully submits these Reply Comments for the FCC's consideration and thanks the Commission for the opportunity to participate in this important proceeding regarding the blocking of robocalls. The comments received in response to the *Declaratory Ruling and Third Further Notice of Proposed Rulemaking* (hereinafter *FNPRM*) provide useful feedback on the Commission's efforts to crack down on unwanted calls and the scourge of illegal robocalls.[1]

The comments reviewed by AARP point to important issues associated with the path forward on the blocking of robocalls. AARP will briefly discuss issues raised by other parties in their opening comments below. AARP finds that there is considerable disagreement among parties on the matter of the appropriate safe harbor. AARP will thus begin this reply with the safe harbor issue.

Safe Harbor

In opening comments, AARP urged the Commission to move conservatively regarding the establishment of a safe harbor, suggesting a "glide path" that would acknowledge the transitional issues associated with implementation of SHAKEN/STIR.[2] Consumer Reports, et al. also notes in comments that during the period before full implementation of SHAKEN/STIR that "It would not be appropriate to block calls solely on the basis that they are unauthenticated at this point, because SHAKEN/STIR is not currently viable for many calls."[3] In a similar vein, Voice on the Net Coalition notes that "until certificate delegation or a trusted carrier registry is adopted as part of the SHAKEN/STIR framework, voice service providers who get their telephone numbers

[1] Because the scope of the *FNPRM* now extends beyond robocalls that are illegal, AARP will conserve notation in these reply comments by referring to unwanted calls and illegal robocalls simply as "robocalls." AARP considers "unwanted calls" to be automatically dialed calls that are made to a consumer who *has not provided prior consent*.
[2] AARP Comments, pp. 10-11.
[3] Consumer Reports, et al. Comments, p. 8.

from wholesale providers won't be able to fully implement SHAKEN or sign calls."[4] Absent the full implementation of SHAKEN/STIR, the risks to large numbers of callers of having their legal calls blocked is too significant to allow a broad safe harbor that would encourage aggressive carrier blocking.[5] Thus, AARP recommends that a narrow safe harbor be adopted. Once SHAKEN/STIR is fully implemented, AARP recommends that the Commission establish a safe harbor that includes the deployment of a call authentication standard like SHAKEN/STIR, or its successor. Regarding the inclusion of "reasonable analytics" in a safe harbor, AARP encourages the Commission to establish "analytics best practices" that could become part of a safe harbor. Any safe harbor should also include robust and no-cost mechanisms for callers who are inappropriately blocked to quickly recover.

AARP observes that service providers such as AT&T, T-Mobile, and Verizon urge the Commission to establish expansive safe harbors.[6] AARP urges the Commission to reject these proposals. AARP is concerned that broad safe harbor provisions will reduce incentives for carriers to exercise care in blocking calls and may result in legal calls being blocked.

SHAKEN/STIR is a key component of compliance for call blocking

AARP and other parties believe that SHAKEN/STIR deployment is a key element of the solution to the robocall problem.[7] AARP and other parties support requirements for the prompt deployment of this technology for all domestic service providers,[8] and hopefully that deployment

[4] Voice on the Net Coalition, p. 3.
[5] Consumer Reports, et al. Comments, p. 8; American Association of Healthcare Managers Comments, p. 5; INCOMPAS Comments, p. 4.
[6] AT&T Comments, pp. 4-5; Sprint Comments, p. 2; T-Mobile Comments, p. 2; Verizon Comments, p. 12.
[7] Comcast Comments, p. 4; CTIA Comments, p. 5; SPRINT Comments, p. 3; TracFone Comments, pp. 3-4; US Telecom Comments, p. 4.
[8] Comcast Comments, p. 10; Consumer Reports, et al. Comments, p. 3; INCOMPAS Comments, p. 14.

will eventually also be on a global basis.[9] AARP views SHAKEN/STIR as desirable not only because of its ability to undermine number spoofing, which provides a solid foundation for the blocking of both illegal and unwanted robocalls, but also due to the standardization of the protocols associated with this blocking technology and the anticipated ubiquitous implementation of the standard. With SHAKEN/STIR the Commission can act with a higher degree of confidence that the resulting blocking will not violate Sections 201(b) and 202(a) of the Communications Act. However, analytics are another matter. Unless the Commission adopts analytic best practices as part of the safe harbor, the Commission cannot be sure that the blocking based on analytics is lawful. Encouraging carriers to aggressively block calls through the use of a "black box" of proprietary analytics is not a reasonable alternative. The Commission should not absolve service providers of the risk that aggressive call-blocking analytics will impose on callers. Finally, as noted above, AARP also believes that, in the period prior to the full implementation of SHAKEN/STIR, the safe harbor provisions should not encourage aggressive blocking of calls. Because many consumers continue to be served by service providers who cannot comply with SHAKEN/STIR, other means of identification of likely robocalls should be employed, such as targeting unsigned calls from entities that do not participate in the Industry Traceback Group.[10]

[9] US Telecom Comments, pp. 13-14.

[10] AT&T notes that recent enhancements made to the traceback process allow a more rapid and accurate identification of illegal robocall traffic (AT&T Comments, pp. 21-22). CTIA states that "Collaborative traceback efforts are uniquely valuable because they help prevent bad actors from using providers' networks and help enforcement entities target those bad actors." (CTIA Comments, p. 6.)

Some service provider safe harbor proposals would encourage overly aggressive blocking

AARP finds that service provider proposals would promote overly aggressive blocking. For example, AT&T proposes a safe harbor that is entirely free from reference to any specific technology or methods, resulting in an overly-broad statement that would free service providers from liability for over-aggressive call blocking.[11] Similarly, Verizon proposes a vague safe harbor with a focus on the use of reasonable analytics that "includes ingesting the SHAKEN/STIR verification."[12]

T-Mobile also states that a broad safe harbor is necessary, but T-Mobile's comments illustrate problems that can arise from a broad safe harbor:

> To encourage these providers to block illegal and unwanted robocalls, on an opt-out basis, the Commission should extend the safe harbor to include blocking based on reasonable analytics. *This is important because, however advanced the analytics used by carriers to block calls, there will always be some risk that legitimate calls are inadvertently blocked.* Absent a safe harbor to manage this risk, carriers will be more likely to offer call blocking on an opt-in basis only, *or else employ more conservative criteria in deciding which calls to block, resulting in more robocalls reaching consumers' devices*.[13]

[11] "A voice service provider that inadvertently blocks a legitimate call shall not be deemed to have violated the Communications Act of 1934, as amended, or the Commission's rules, if, at the time the provider blocked the call, the provider:

> (a) performed network blocking of calls in connection with an event that the provider had a good-faith reason to believe was an illegal robocall event;
>
> (b) had procedures in place for network blocking that were reasonably likely to confirm that calls blocked were limited to illegal robocalls;
>
> (c) followed those procedures; and
>
> (d) had a process in place to unblock legitimate calls in the event of any inadvertent blocking of such calls." AT&T Comments, p. 12.

[12] Verizon Comments, p. 11.

[13] T-Mobile Comments, pp. 8-9, emphasis added.

T-Mobile admits that "advanced analytics" will result in the blocking of legitimate calls, and there can be little doubt that analytics that are not as advanced as those envisioned by T-Mobile will block even more legitimate calls. AARP also believes that T-Mobile is creating a false dilemma when it states that absent analytics "more robocalls" will reach customer devices. For this to be true the full implementation of SHAKEN/STIR would need to have no impact on the robocall problem, which AARP believes is unrealistic. If T-Mobile believes that full implementation of SHAKEN/STIR will exacerbate the robocall problem, or leave it unchanged, then T-Mobile should provide evidence to that effect.

Some service providers offer a more restrained view of the safe harbor. For example, Comcast supports the NPRM's proposal for a safe harbor "for voice providers that block calls (or a subset of calls) that fail Caller ID authentication under the SHAKEN/STIR framework."[14] Sprint also proposes a safe harbor that offers some specifics regarding the adoption of SHAKEN/STIR, participation in the Industry Traceback Group, and the creation of a challenge and redress mechanism for false positive errors. In an environment where SHAKEN/STIR were fully implemented, AARP finds Comcast and Sprint's proposals to be more reasonable. However, until SHAKEN/STIR is ubiquitous, even Sprint's safe harbor could encourage overly aggressive blocking.

AARP believes that until SHAKEN/STIR is fully implemented by domestic carriers, any safe harbor adopted by the Commission must be conservative. If it is the case that "analytics" is an essential step in blocking illegal calls, then the Commission should work to establish best practices for the analytics prior to those analytics being included in any safe harbor. As the

[14] Comcast Comments, p. 5.

FNPRM notes, analytics may be based on a variety of factors.[15] Should the Commission want to establish a safe harbor that includes the use of analytics, then it should identify the best practices associated with analytics and shape the safe harbor around those best practices.

The Commission should establish a balanced safe harbor that will promote reasonable blocking technology deployment that protects consumers from illegal and unwanted robocalls and also protects legitimate callers from blocking, while also allowing those who may be inadvertently blocked to quickly recover at the lowest cost possible.

"Reasonable analytics" best practices should be established by the Commission

The advantage of the SHAKEN/STIR approach is that it provides a standardized method for the identification of calls that are likely to be illegal.[16] Moving beyond SHAKEN/STIR to blocking methods based on analytics will increase the degree of subjectivity in call blocking. Unreasonable call blocking analytics could result in widespread suppression of legal calls.

As noted by INCOMPAS, many types of legal calls that are likely to be wanted by consumers are also likely to have characteristics that will be negatively flagged, and possibly blocked, by analytics.

> In addition to numbers for emergency services, one of the most well known forms of wanted robocalls are notification services, which can be critical in nature. School messaging, medical notifications, valid conferencing, and similar important services may unfortunately fall under the "reasonable analytics" criteria for blocking adopted in the Declaratory Ruling. Since these calls are typically short in duration, done in bursts, and sent to large, local communities, they are likely to be flagged. This increases the likelihood that these services may be blocked or have their attestation degraded, despite the fact that they are clearly valued by consumers who depend on them for vital information.[17]

[15] *NPRM,* ¶35.
[16] *FNPRM,* ¶50.
[17] INCOMPAS Comments, p. 11.

Likewise, Boulder Regional Emergency Telephone Service Authority states:

> Emergency Notification Service ("ENS") involves autodialing all landline telephones located within a defined geographic area, and all wireless (portable or nomadic phones) registered to addresses within the defined geographic area; and delivering a prepared or pre-recorded message. Many ENS providers maintain geographically distributed facilities from which ENS calls can be placed. ENS calls may also present a caller-number and caller ID associated with agency (*sic*) which initiates the calls. ENS calls are thus robocalls, are intended to be transmitted from different locations than that of the agency causing the ENS calls to be transmitted, may provide caller numbers and caller IDs of the agency causing the ENS calls to be transmitted rather than of the ENS provider, and may appear the same as the marketing and fraudulent robocalls which the Commission seeks to prevent.[18]

These observations point to the importance of the analytics deployed by a service provider relying on best practices.

On the matter of deploying call-blocking analytics AT&T notes:

> AT&T' s unique call-blocking program provides the basis for this broad safe harbor proposal, *and can be used as a model for other providers to target and work to eliminate suspected illegal calls*. At the network level, AT&T blocks calls that—after thorough analysis and investigation—AT&T's global fraud team reasonably determines are illegal. Under this program, AT&T compiles into a suspected robocall report aggregate call data that informs the detection of suspicious calls. As previously detailed in the record, these data include, but are not limited to: average call duration data, call completion rates, CNAM values, call volumes and the timeframes in which calls are placed, complaint data (including Commission and Federal Trade Commission ("FTC") complaint data), sequential dialing patterns, and call volumes to telephone numbers on the FTC's Do Not Call list. The report is updated on a virtually continuous basis. Based on the information in the suspected robocall report, AT&T investigates suspect telephone numbers, including but not limited to, a fraud investigator dialing the telephone number, and implements blocks on particular telephone numbers where there is reasonable basis to believe the call is illegal.[19]

AARP encourages the Commission to take up the challenge implicit in AT&T's proposal—defining analytic best practices to be included in a safe harbor. AT&T indicates that its unique call-blocking program can be used as a model for other providers, and AARP commends AT&T

[18] Boulder Regional Emergency Telephone Service Authority Comments, p. 1.
[19] AT&T Comments, pp. 13-14.

for its willingness to share its expertise. The Commission should extend the rulemaking process to encourage input from all parties on the matter of best practices for call-blocking analytics. AT&T and other parties with expertise in call blocking analytics can contribute, with the end result being a set of best practices for call blocking analytics. Those analytic best practice standards could then be used in a safe harbor. Until the Commission establishes just what "reasonable analytics" are, the safe harbor provisions should not include this currently undefined term.[20]

"Analytic best practices" need not define specific methodology

AARP appreciates that the game of cat and mouse between service providers and illegal robocallers will result in the need for service provider innovation with regard to blocking, and evolving analytics will need to play a role in carrier efforts to block illegal calls. Sprint is correct when it states:

> The Commission should not attempt to narrowly prescribe a methodology carriers and analytics entities must use to determine whether a call is legal or illegal, wanted or unwanted. The technology to identify illegal and unwanted calls is rapidly evolving, and bad actors rapidly change their calling practices in response. Any attempt to define what criteria indicate an illegal or unwanted call will likely be immediately obsolete.[21]

However, the Commission can establish a best practices foundation for "reasonable analytics" without narrowly prescribing methodology. Service provider risks can be reduced (and innovation encouraged) if service providers also provide free, rapid, and reliable mechanisms for customers who are inappropriately blocked to recover, and such a mechanism should be included

[20] Adopting standardized call analytics standards would not preclude carriers from developing additional methods to block calls based on analytics. The fact that those methods would fall outside of the safe harbor would encourage those carriers to exercise caution with more aggressive blocking technologies.
[21] Sprint Comments, p. 3.

in any safe harbor. An efficient and effective recovery mechanism would appropriately reduce risks faced by consumers.

The real risk of false positives requires mechanisms for consumers to quickly recover at no charge

In open comments, AARP raised the issue of false positives and the need to discourage blocking of legitimate callers.[22] Many other parties point to risks of false positives.[23] AARP also observes that the risks of false positives are confirmed by service providers who acknowledge that false positives will be a fact of life with the new blocking PSTN. For example, Verizon notes that even with the most sophisticated call blocking analytics "errors do occur."[24] T-Mobile states that it is already addressing the false positive problem by providing tools to its customers who are adversely affected.[25] AT&T provides an important description of the problems that it expects as call blocking technology is deployed:

> AT&T expects that technical network-related errors will be responsible for most, if not all, instances in which SHAKEN/STIR verification fails—particularly in the early days of implementation ahead of the existence of a complete administrative framework—not because the calling party spoofed the originating telephone number or attempted to subvert the SHAKEN/STIR process. *And such "failures" are to be expected as implementation proliferates and providers continue to learn from the individualized provider-to-provider implementations. Thus, for these and potentially other reasons, a call that fails SHAKEN/STIR verification may be perfectly legitimate and, in fact, wanted by the receiving party*.[26]

[22] AARP Comments, p. 2.
[23] American Association of Healthcare Management Comments, p. 4; ACA International Comments, p. 10; American Bankers Association Comments, p. 5; CTIA Comments, p. 17; INCOMPAS Comments, p. 8; Larimer Emergency Telephone Authority Comments, p. 2; NTCA Comments, p. 14; SiriusXM Comments, p. 6.
[24] Verizon Comments, p. 12.
[25] T-Mobile Comments, p. 9.
[26] AT&T Comments, p. 8, emphasis added.

Thus, it is abundantly clear that false positives will be a real problem for an extended period. The Commission must ensure that service providers have effective and efficient mechanisms in place to enable rapid and cost-free recovery for those callers who are inappropriately blocked.[27]

A critical calls list generates complex issues

AARP continues to strongly support the need to protect critical calls, however, the complexity of this matter is illustrated in the comments of many parties. AARP encourages the Commission to move with caution on the matter of establishing a critical calls list.[28]

CTIA observes that "protecting critical calls must be a priority for voice service providers, especially as they more aggressively deploy call-blocking tools based upon reasonable analytics."[29] This comment links the importance of a properly defined safe harbor and the protection of critical calls. AARP is concerned that the aggressive blocking of calls based on analytics that are said to be "reasonable" by service providers will lead to the inappropriate blocking of calls that may be critical, or just lawful. As discussed above, establishing a conservative safe harbor that uses a "glide path" approach is a more reasonable approach.

The scope of the critical call list raises important questions as to how to define a "critical call." For example, Heartland Credit Union Association proposes that critical calls should include "fraud alerts, data breach notifications, remediation messages, utility outage notifications, product recall notices, prescription notices, and mortgage servicing calls required by Federal or State law."[30] Consumer Reports, et al. offer an alternative perspective on critical calls:

[27] American Association of Healthcare Administrative Management Comments, p. 5; ACA International Comments, p. 10; American Bankers Association Comments, p. 5; NTCA Comments, p. 14.
[28] AARP Comments, p. 11.
[29] CTIA Comments, p. 19.
[30] Heartland Credit Union Association Comments, p. 1.

> No private businesses should be on the critical calls list. Phone numbers used by local public schools to alert parents of school emergencies may be added to the generic white list. But calls from those numbers should be limited to real emergencies. Calls from schools that provide reminders of upcoming conferences, or band rehearsals, etc. should not be included on the critical calls list.[31]

Consumer Bankers Association urges the Commission to expand the critical calls list to include "fraud alerts, low balance notifications, and data breach notifications."[32] Combined, AARP believes that these requests generate an overly expansive set of "critical calls." On the other hand, AARP finds merit in T-Mobile's observation that "calls from PSAPs may be an appropriate starting point since they represent a known and verifiable category of entities for which no blocking may be reasonably implemented. Expanding the category of critical calls beyond PSAPs will present definitional challenges that will make not blocking problematic, unwieldy, and subjective."[33]

It is clear from these comments that protection of critical calls is important, but that the definition of what is a critical call must be carefully crafted. AARP believes that the Commission should limit critical calls at this time to those associated with PSAPs and consider future expansion of the definition of critical calls in response to problems that emerge.

Any critical calls list should be protected

AARP also believes that the critical calls list would require a high degree of protection, as illegal robocallers could easily disrupt both the usefulness of call blocking efforts and the usefulness of emergency services if the critical calls lists were to fall into the wrong hands.[34] Thus, minimizing the number of entities that access the critical calls list will be essential, and

[31] Consumer Reports, et al. Comments, p. 9.
[32] Consumer Bankers Association Comments, page three of four.
[33] T-Mobile Comments, p. 10.
[34] Comcast Comments, pp. 12-13; LETA Comments, p. 5; US Telecom Comments, p. 10.

protecting the list with state-of-the-art security measures is equally important. However, limiting the number of individuals with access may be difficult. Ensuring that all critical numbers are on the list requires the input of parties at the local, state, and national level, and implementing that review while maintaining security will be challenging. For example, the Massachusetts Department of Telecommunications and Cable proposes that state commissions be allowed to review critical calls lists in their jurisdictions prior to those lists being adopted.[35] An even more expansive access to the Critical Calls List is envisioned by the Larimer Emergency Telephone Authority, which states:

> The proposed Critical Calls List should be an upload process through a secure portal by a 9-1-1 governing body, PSAP, or Federal/State/Local government emergency-related agency and their Emergency Alert System vendors. The process should allow for subsequent additions/edits/deletions to their entries by a 9-1-1 governing body, PSAP, or Federal/State/Local government emergency-related agency and their Emergency Alert System vendors.[36]

Given that there are over 6,000 PSAPs in the U.S., a large number of entities would have access to the critical calls list under this proposal. Alternatively, at least one party proposes that the critical call list be available to entities outside of government and/or the PSAP community. The App Association, an organization that represents "approximately 5,000 small business software application development companies," advocates for that list being centralized and available to all App Association members.[37] The degree of access suggested by these parties could be problematic. The Commission will face significant challenges in keeping the critical calls list secure. In summary, commenters propose, possibly for good reason, that the critical calls list be

[35] MDTC Comments, p. 7.
[36] LETA Comments, p. 3.
[37] App Association Comments, p. 6.

centralized and accessible to a number of entities. However, the greater the number of entities that can access the critical calls list, the greater the security challenges.[38]

AARP urges the Commission to initially limit the number of calls that are defined as critical and to adopt T-Mobile's recommendation that the initial critical calls list targets calls originating from PSAPs. The Commission should also limit access to the databases associated with critical calls and ensure the security of any critical calls list it establishes.

"Unwanted calls" should be clearly defined by the Commission

The *FNPRM* expanded the scope of blocking to include "unwanted calls."[39] However, as noted by Commissioner O'Rielly, the terms "wanted" and "unwanted" calls are vague and subjective.[40] In opening comments, AARP suggested that unwanted calls be defined as those automatically dialed calls that are made to a consumer who has not provided prior consent.[41] Other parties pointed to the need for the Commission to better define unwanted calls.[42] AARP encourages the Commission to define unwanted calls as AARP suggests as this will inform service providers as they endeavor to block both illegal and unwanted calls.

Blocking and unblocking should be free of charge

In comments, AARP emphasized that the successful implementation of robocall blocking technology requires that the blocking technology be available to consumers at no charge. Blocking that is available to all consumers will generate a more robust blocking solution.[43] AARP finds that other parties also emphasize the importance of no-cost blocking services.

[38] CTIA Comments, p. 21; Ring Central Comments, p. 8; USTA Comments, p. 10; Comcast Comments, pp. 12-13.
[39] *FNPRM¸ passim.*
[40] *FNPRM,* Comments of Commissioner O'Rielly.
[41] AARP Comments, p. 1.
[42] Competitive Carriers Association Comments, p. 3; Consumers Bankers Association, page two of four.
[43] AARP Comments, p. 9.

Massachusetts Department of Telecommunications and Cable states that "the FCC should require that call-blocking programs be free to consumers."[44] Consumer Reports, National Consumer Law Center, et al. also support blocking services that are free of charge.[45] The American Bankers Association, et al. state that "Voice Service Providers also should remove an erroneous block within 24 hours of learning of the block, at no charge to the caller."[46] Free unblocking services are also supported by the American Association of Healthcare Administrative Management, ACA International, and Consumer Bankers Association.[47] AARP commends T-Mobile for offering its existing robocall blocking solutions to its customers "free of charge."[48]

Conclusion

AARP appreciates the challenges facing the Commission when enabling the modification of the PSTN to include the blocking of robocalls. AARP urges the Commission to move with caution and to take measures that will protect the integrity of call completion for legal callers, protect those who are inappropriately blocked, and deliver best blocking practices. The recommendations contained in AARP's opening comments and this reply will promote an appropriate balance for these objectives.

[44] MDTC Comments, p. 6.
[45] Consumer Reports, et al. Comments, p. 7.
[46] American Bankers Association, et al. Comments, p. 6.
[47] American Association of Healthcare Administrative Management Comments, p. 6; ACA International Comments, p. 10; Capio Comments, page four of four; Consumer Bankers Association, page three of four.
[48] T-Mobile Comments, p. 4.